

LAW AND DIGITAL TECHNOLOGIES
ELECTRONIC COMMUNICATIONS

ePrivacy

Prof. Gerrit-Jan Zwenne
February 9th, 2022



1

HOME > EU DATA PROTECTION > COUNCIL OF THE EU RELEASED A (NEW) DRAFT OF THE EPRIVACY REGULATION

Council of the EU Released a (New) Draft of the ePrivacy Regulation

By Dan Cooper and Anna Oberschelp de Menezes on January 6, 2021
POSTED IN DATA PRIVACY, EU DATA PROTECTION, EUROPEAN UNION, GDPR


On January 5, 2021, the Council of the European Union released a new **draft version** of the ePrivacy Regulation, which is meant to replace the ePrivacy Directive. The European Commission approved a first draft of the ePrivacy Regulation in January 2017. The draft regulation has since then been under discussion in the Council.

On January 1, 2021, Portugal took over the presidency of the Council for six months. Ahead of the next meeting of the Council's working party responsible for the draft ePrivacy Regulation, the ~~Portuguese~~ **Portuguese** Presidency issued a revised version of the draft regulation. This is the **14th draft version** of the ePrivacy Regulation (including the European Commission's first draft).

Once approved, the ePrivacy Regulation will set out requirements and limitations for publicly available electronic communications service providers ("service providers") processing data of, or accessing devices belonging to, natural and legal persons "who are in the [European] Union" ("end-user"). The regulation aims to safeguard the privacy of the end-users, the confidentiality of their communications, and the integrity of their devices. These requirements and limitations will apply uniformly in all EU Member States. However, EU Member States have the power to restrict the scope of these requirements and limitations where this is a "necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests."



2



Council of the
European Union

Brussels, 5 January 2021
(OR. se)

5008/21

LIMITE

TELECOM 1
COMPET 1
MI 1
DATAPROTECT 1
CONSOM 1
JAI 1
DIGIT 1
FREMP 1
CYBER 1
CODEC 3

Interinstitutional File:
2017/0003(COD)

NOTE

From: Presidency

To: Delegations

No. prev. doc.: 9931/20

No. Clon doc.: 5358/17


Subject: Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

INTRODUCTION

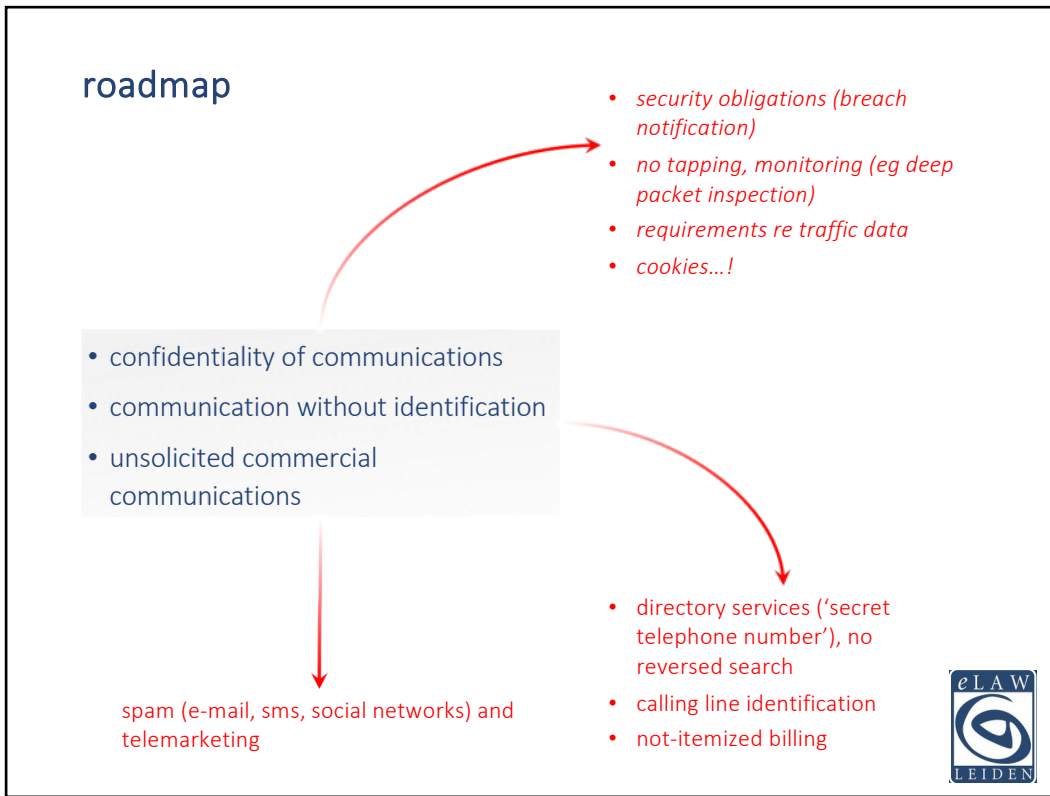
1. In view of the WP TELE meeting on 7 January, Delegations will find in Annex I the Presidency proposal of the ePrivacy Regulation.
2. The Presidency aims to conduct swift discussions with Member States, intending to jointly discuss articles and the relevant recitals.
3. During the recent discussions in the WP TELE, it has become clear that the majority of Delegations could not support the text as it stood in doc. 9931/20. A number of them expressed their wish for more substantial changes in the proposal.

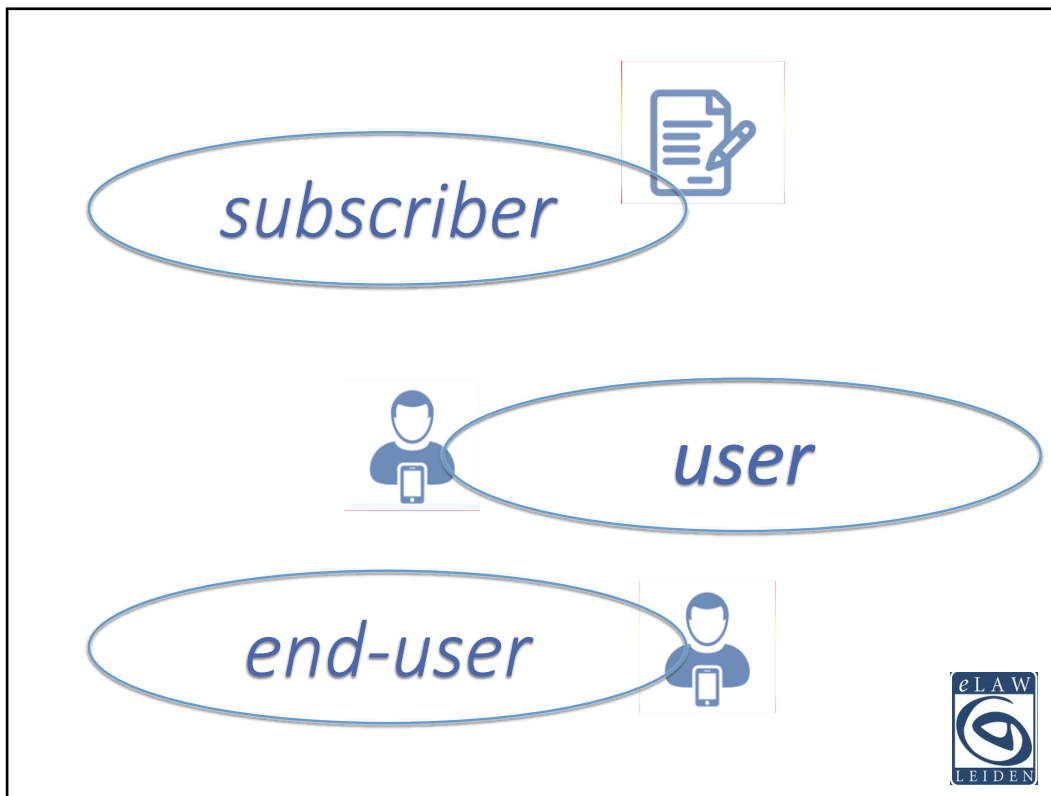
5008/21
TREE.L.B.
PB/vk
1

LIMITE
EN



3






5

This block features a large, circular, blue stamp with the word 'CONFIDENTIAL' repeated twice around the perimeter and a central banner with the word 'CONFIDENTIAL' in bold, white letters. Below the stamp, the text 'confidentiality of communications' is written in a dark blue, sans-serif font. A small 'eLAW LEIDEN' logo is positioned in the bottom right corner.


6




security obligation

appropriate technical and organisational measures to safeguard security of the [electronic communication] services, if necessary in conjunction with the provider of the public communications network with respect to network security

having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.




7



breach notification

- notify the personal data breach to the competent national authority
- also notify the subscriber or individual, if likely to adversely affect the personal data or privacy of a subscriber or individual, of the breach without undue delay

*24 hours? 72 hours?
what's the startingpoint?*



8

breach notification to DPA

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority [...], unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons

notification to data subject

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.



9

Meldloket datalekken Autoriteit Persoonsgegevens

Een nieuwe melding indienen

Aard van de melding

Wettelijk kader van de melding

Algemene informatie en contactpersoon

Gegevens over het datalek

Verzamelen naar aanleiding van het datalek

authentication...?

10

Art. 6 EPR Art. 5(1) ePD

“electronic communications metadata”


confidentiality of communications and traffic data

no listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned

deep packet inspection (“dpi”)

net neutrality debat...

spam filter...?




The slide features a diagram with two overlapping ovals at the top labeled 'Art. 6 EPR' and 'Art. 5(1) ePD'. A red arrow points from the 'Art. 6 EPR' oval to the text '“electronic communications metadata”'. Another red arrow points from the 'Art. 5(1) ePD' oval to the text 'deep packet inspection (“dpi”)'. A third red arrow points from the 'deep packet inspection (“dpi”) text to the text 'net neutrality debat...'. A fourth red arrow points from the 'net neutrality debat...' text to the text 'spam filter...?'. The main text 'confidentiality of communications and traffic data' is in bold, followed by a paragraph of text. The eLAW LEIDEN logo is in the bottom right corner.

11

Art. 6 ePD

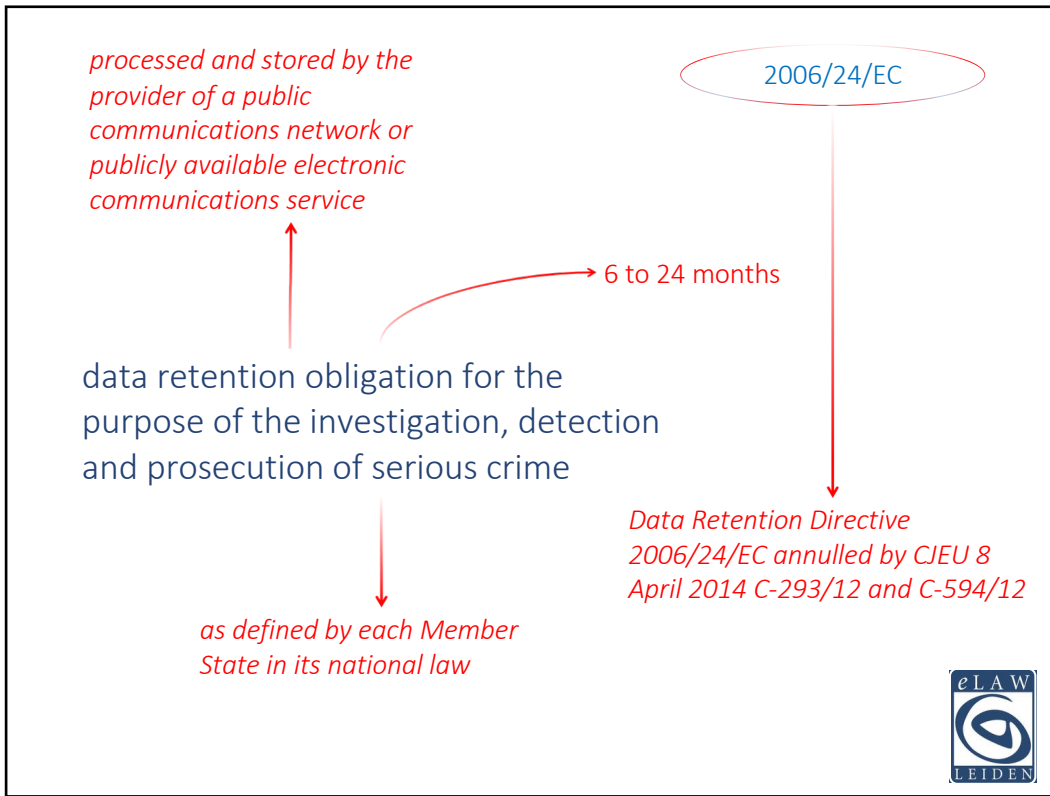
traffic data relating to subscribers and users must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication

with user or subscriber data may be used for the purpose of marketing electronic communications services or for the provision of value added services.

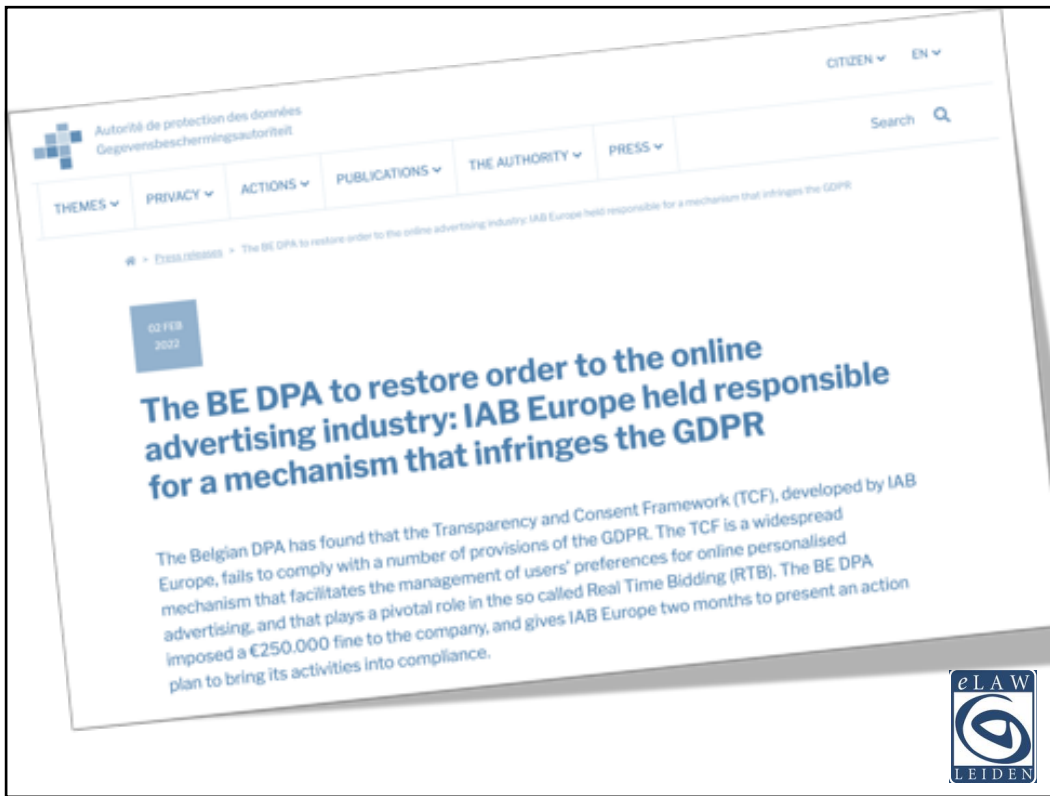


The slide features a diagram with an oval at the top labeled 'Art. 6 ePD'. A red arrow points from the 'Art. 6 ePD' oval to the text 'with user or subscriber data may be used for the purpose of marketing electronic communications services or for the provision of value added services.'. The main text 'traffic data relating to subscribers and users must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication' is in bold. The eLAW LEIDEN logo is in the bottom right corner.

12



13



14




Main findings : the TCF implies the processing of personal data

Contrary to IAB Europe's claims, the Litigation Chamber of the BE DPA found that IAB Europe is acting as a data controller with respect to the registration of individual users' consent signal, objections and preferences by means of a unique Transparency and Consent (TC) String, which is linked to an identifiable user. This means that IAB Europe can be held responsible for possible violations of the GDPR.

The BE DPA identified a series of GDPR infringements by IAB Europe :

- **Lawfulness** : IAB Europe failed to establish a legal basis for the processing of the TC String, and the legal grounds offered by the TCF for the subsequent processing by adtech vendors are inadequate;
- **Transparency and information of the users** : the information provided to users through the CMP interface is too generic and vague to allow users to understand the nature and scope of the processing, especially given the complexity of the TCF. Therefore it is difficult for users to maintain control over their personal data;
- **Accountability, security and data protection by design/by default** : In the absence of organisational and technical measures in accordance with the principle of data protection by design and by default, including to ensure the effective exercise of data subject rights as well as to monitor the validity and integrity of the users' choices, the conformity of the TCF with the GDPR is not adequately warranted nor demonstrated;
- **Other obligations pertaining to a controller processing personal data on a large-scale**: IAB Europe has failed to keep a register of processing activities, to appoint a DPO and to conduct a "DPIA" (data protection impact assessment).



15


Art. 8 ePR Art. 5(3) ePD

cookies! device fingerprinting, pixels etc..

the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information

but functional or technical cookies are allowed nevertheless

“cookies”



16

where technically possible and feasible [...] consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet.




17

Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment



18



CNIL.
To protect personal data, support innovation, preserve individual liberties

MY COMPLIANCE TOOLS | DATA PROTECTION | TOPICS | THE CNIL | Q | TW

🏠 > Cookies and other tracking devices: the Council of State issues its decision on the CNIL guidelines



🔍 🖨️ 📄

Cookies and other tracking devices: the Council of State issues its decision on the CNIL guidelines

29 June 2020

In its decision of 19 June 2020, the Council of State (Conseil d'État) essentially validated the guidelines on cookies and tracking devices adopted by the CNIL on 4 July 2019. The purpose of these guidelines was to clarify the enhanced legal

GDPR. However, the Council of State overturned the provision of the guidelines prohibiting in a general and absolute manner the practice of "cookie walls", ruling that such a prohibition could not be included in an act of soft law. The CNIL takes note of this decision and will adjust its guidelines and future recommendations to comply with it accordingly.

19



CNIL.
To protect personal data, support innovation, preserve individual liberties

MY COMPLIANCE TOOLS | DATA PROTECTION | TOPICS | THE CNIL | Q | TW

🏠 > Cookies and other tracking devices: the Council of State issues its decision on the CNIL guidelines

🔍 🖨️ 📄

The Council of State's position on cookie walls

However, in its decision of 19 June 2020, the Council of State suppressed a paragraph in which the CNIL considered that the Internet user should not suffer major inconvenience in the event of the absence or withdrawal of consent. The CNIL considered in particular that access to a website could never be subject to the acceptance of cookies ("cookie walls").


The CNIL had followed the doctrine of the European Data Protection Board (EDPB), which brings together all the European data protection authorities, which has considered, until recently, that in order for consent to be freely given, access to services and functionalities must not be made conditional on the consent of a user to the storing of information, or gaining of access to information already stored, in the terminal equipment of a user (so-called cookie walls) (Guidelines on consent under GDPR of 4 May 2020).

The Council of State considered that by deducting this general prohibition from the GDPR, the CNIL had gone beyond what is legally possible with guidelines, which are an instrument of "soft law".

The Commission takes note of the Council of State's decision and will comply strictly with it.




20



3aa) Making access to website content provided without direct monetary payment dependent on the consent of the end-user to the storage and reading of cookies for additional purposes **would normally not be considered** as depriving the end-user of a genuine choice if the end-user is able to choose between services, on the basis of clear, precise and user-friendly information about the purposes of cookies and similar techniques, between an offer that includes consenting to the use of cookies for additional purposes on the one hand, and an equivalent offer **by the same provider** that does not involve consenting to data use for additional purposes, on the other hand. Conversely, in some cases, making access to website content dependent on **consent to the use of such cookies** may be considered, in the presence of **a clear imbalance** between the end-user and the service provider as depriving the end-user of a genuine choice. This would normally be the case for websites providing certain services, such as those provided by public authorities. Similarly, such imbalance could exist where the end-user has only few or no alternatives to the service, and thus has no real choice as to the usage of cookies for instance in case of service providers in a dominant position.


21

Article 8

Protection of end-users' terminal equipment information stored in terminal equipment of end-users and related to or processed by or emitted by end-users' terminal such 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:

(g1) it is necessary for a purpose other than that for which the information have been collected under this Regulation. Where it is not based on the end-user's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 11 the person using processing and storage capabilities or collecting information processed by or emitted by or stored in the end-users' terminal equipment shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the electronic communications data are initially collected, take into account, inter alia:



22

communication without identification



23

subscriber has the right to have invoice without details



non-itemized billing

calling line identification

directory services



- *subscriber must be informed about inclusion in directories (incl purposes), and*
- *provided a choice (opt-in or opt-out)*

Art. 7, 8 and 12 ePD



user has the right to

- *block cli-presentation of his/her own calls*
- *reject cli-blocked calls from others*
- *block cli-presentation of calls from others*

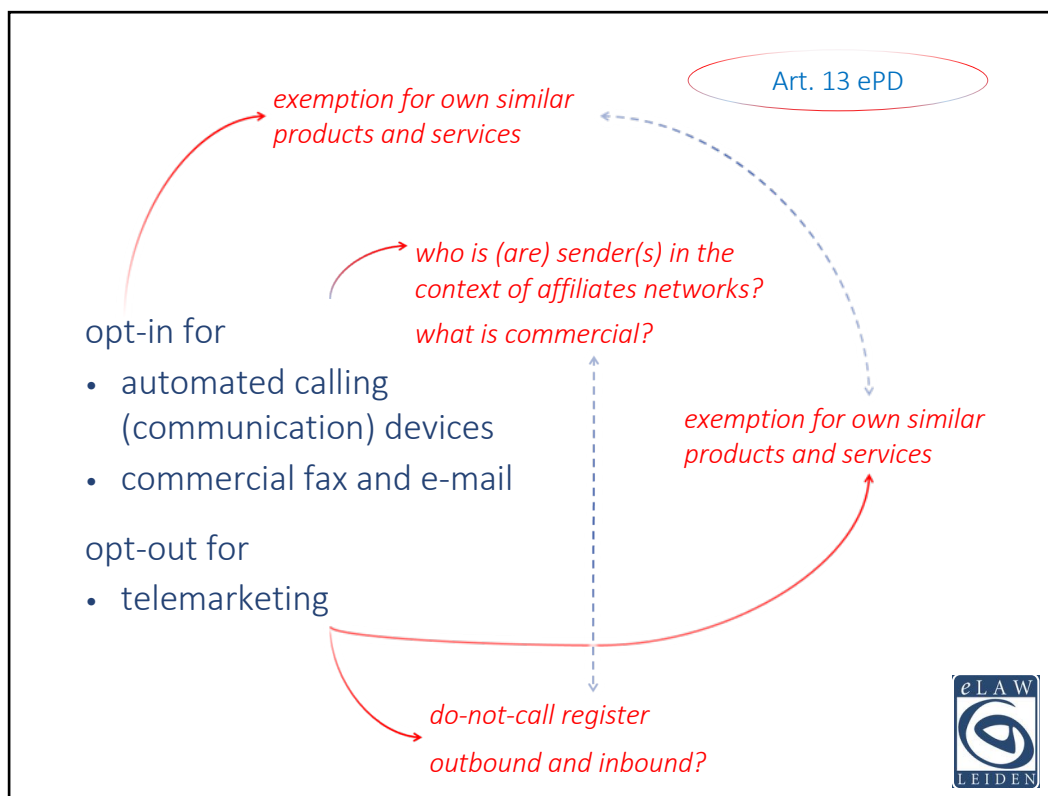


24

unsolicited commercial communication



25



26

questions?

g.j.zwenne@law.leidenuniv.nl

