Axel Voss
Member of the European Parliament

(A) My main arguments/concerns against the current ePrivacy-proposals

1. **Legal uncertainty / excessive scope**: If we are going for an ePrivacy regulation as „lex specialis“, our present main instrument for protecting personal data - the GDPR - is just valid when there is a special reference to it. This means that we do not have a coherent legal system any longer. Its relation to the GDPR will create enormous uncertainties for citizens and businesses in practice. This is exacerbated by the fact that the ePrivacy regulation breaks with the risk based approach of GDPR, which implements the principle of accountability: this is absent from the tick-the-box ePrivacy. This is all the more regrettable that the GDPR aims at creating a real culture of data protection, where businesses are more responsible and accountable for each of their data processing operations. If we do not continue this approach in ePrivacy, we lose the benefits of GDPR. The main objective of the old ePrivacy directive was to protect the confidentiality of communication. Now, we are protecting citizens against all (alleged) risks. In Article 1 of the new proposal, the scope is extended massively and includes the protection of personal data while processing. So far, this area was solely regulated by the GDPR. In my opinion, we should therefore give the GDPR a chance to work properly. In the end, we will maybe even realize that the ePrivacy regulation is not needed at all and that we can just add a principal such as “communication should be confidential” to the GDPR.

2. **Detrimental to innovation**: If data cannot be processed or cannot be further processed, the „Free Flow of Data principle“, a goal for the European approach to digitalization, is not valid any longer. A general ban of processing communication data would not only prevent many current digital services from working properly, it would also interfere massively with innovation. This means innovations of services or products (real-time translation, text into pictures, pictures into text, voicing / texting developments for disabled person, holography etc.) are hampered! Self-learning algorithms need lots of data to learn but cannot learn any longer and as a result, artificial intelligence cannot be developed in Europe in a competitive way to Asia or America. The planned restrictions on WLAN, Bluetooth, IoT and M2M-communications would prevent, for instance, the effective realization of Smart Cities, Smart Traffic, digitalisation of industry and Smart Buildings concepts.

3. **Consent for the processing of data in article 6**: The ePrivacy proposal demands a mutual consent for processing communication data, meta-data and content. As consequence, many modern services would not work anymore. Three examples: (a) telecommunication operators could not carry out big data analytics and thus, could not provide traffic maps, measure energy consumption or detect the spread of epidemics (b) internet provider could no longer scan content by automatic means in order to provide assisting services based on machine-learning (e.g. translator) or to detect malware as well as child sexual exploitation material (c) mail provider would need to request a consent by a third-party-recipient before they can send him the email from their costumer. Therefore and in general, we should refrain from focusing on consent too intensively, as it is no longer a functioning approach. On the contrary, concepts such as transparency, data sovereignty, opt-out solutions, rights of objection as well as a new category of data (e.g. pseudonymised data) or at least better differentiation between anonymised, pseudonymised and encrypted data would be a much better solution and are already provided for in GDPR.

4. **Ban of third party cookies in article 8**: If we are not allowing „third party cookies“ anymore, existing business models based on targeted advertising cannot go on and we will create (European) unemployment. At the same time, we are allowing the (American) browser software to control the

internet as sole gatekeepers and are thus supporting their monopolies. This is the exact opposite of what we actually want. There is no reason at all for not allowing businesses based on third-party-cookies to continue their work from a data protection point of view. They have to follow the same data protection rules as all other data companies!

5. **Unnecessary time pressure**: European enterprises as well as start-ups are currently trying to adapt their business models to the new GDPR-rules that come into force on 25 May 2018. With the ePrivacy regulation, which according to Article 29 should entry into force on the same day, they would face another highly complex legal framework that has profound consequences for their daily business. Many additional adjustments would be necessary - a complicated process that normally takes up to 18 months. I am relieved that - due to the delay in the Council - the 25 May 2018 is no longer realizable for the ePrivacy regulation. However, the fact that the GDPR as well as the ePrivacy regulation follow each other very closely means that the European industry will need to make a multitude of new adjustments in a very short period. This is not realistic and at the same time causes the risk of high penalties for the industry! A point that - again - is much more problematic for (European) SMEs than for powerful (American) internet companies.

(B) Proposals for Article 6 (version of the Commission) to enable ‘further processing’

It is crucial to have the possibility to process relevant data further! In order to facilitate a ‘further processing’ of communication data, metadata and communication content, different approaches / levels of data protection are thinkable. Based on my latest compromise proposals on Article 6 (version of the Commission) in the JURI committee, I see the following options:

OPTION 1: adapt Art 6 (1) a-f GDPR for the ePrivacy regulation

OPTION 2: like Option 1 but replace ‘legitimate interest’ in Art 6 (1) f) with ‘further processing’

OPTION 3: Option 2 + ‘pseudonymised or anonymised data’ as in Art 6 (4) GDPR

OPTION 4: Option 3 + plus an additional impact assessment (Art 35 GDPR)

OPTION 5: Option 4 + a further reference to Art 40 and following in the GDPR, meaning either:

a) Certification by the DPA‘s OR binding corporate rules OR a code of conduct
b) Certification and binding corporate rules
c) Certification and code of conduct