Brussels, 5 June 2018

Council of the European Union
Transport, Telecommunications and Energy Council Configuration Ministers
Rue de la Loi 175 - 1048 Brussels, Belgium

RE: 8 June TTE Council – Policy debate on the progress of negotiations on the draft ePrivacy Regulation

Dear Ministers,

I am writing to you on behalf of BSA | The Software Alliance[i] ("BSA"), the leading advocate for the global software industry, regarding the upcoming EU Telecommunications Council ("TTE Council") meeting where the status of technical deliberations on the draft **ePrivacy Regulation ("ePR")** will be discussed. BSA members share a **deep commitment to protecting the confidentiality of communications** and consequently, we have been closely following the work of the Working Party on Telecommunications and Information Society ("WP TELE") on the draft ePR ahead of this week's Ministerial policy debate.

While we recognise the hard work of the WP TELE over the past months, we firmly believe that the recent Bulgarian Council Presidency compromise text fails to reach the proper balance between the protection of the principle of confidentiality and allowing for continued digital innovation (see Annex). As noted in numerous sections of the Bulgarian Council Presidency's Progress Report (Doc 8917/18), we believe that **more reflection amongst Member States is needed on the draft ePR to ensure a coherent legal framework for the EU**. With the General Data Protection Regulation ("GDPR") having only recently entered into force, the ePR should be used as a way to address any gaps presented by the newly enacted framework in an effort to provide continued legal clarity for businesses and citizens alike.

More specifically, we are becoming increasingly concerned that the debate **continues to confuse the concept of *data protection*** (regulating the processing of data related to individuals) **with *confidentiality*** (protection of communications from unauthorised access by third parties). These rights are intentionally separated in the EU Charter of Fundamental Rights (Article 7 and 8) and that same separation should be reflected in both legal instruments. The GDPR should comprehensively provide for data protection, while the **ePR should focus solely on protecting the confidentiality of communications.**

We therefore encourage you to **reject the calls to provide the Bulgarian Council Presidency with a mandate to begin informal trilogue negotiations** during Friday's TTE Council and to take further steps to ensure that the Council crafts a workable position on the draft ePR. Trilogue negotiations should only commence once a robust, balanced and comprehensive Council General Approach is obtained. We call on Ministers to not only think of how to regulate today's technology, but also to consider how the draft ePR can be improved to *enhance* the creation of future technologies.

Sincerely,

Thomas Boué – Director General, Policy – EMEA

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

ANNEX – Questions for the Policy Debate at the TTE Council of 8 June 2018

Question 1 – Do you think that the current approach as proposed by the Presidency and set out above on the permitted processing of metadata (art 5 and 6) is an acceptable basis to move forward? What other improvements could be made?

BSA remains deeply concerned with the Presidency's overall proposals for Articles 5 and 6. In combination, these articles will **significantly constrain the ability for companies to innovate and improve their services in Europe**. Many services depend on the use of large-scale data sets to develop their features over time – it is not always possible for organisations to obtain consent from all relevant end-users, or alternatively, to improve features using the data from a small sub-set of users. Without the ability to use data to improve products and services, **innovation will shift to other markets around the globe**.

Articles 5 and 6 should be amended to allow for expanded us of both meta and content data, subject to robust safeguards. Article 6 should have a broader permission for the use of metadata to improve services, subject to appropriate protections for user's information. In addition, Article 6 should also provide for the **use of content data for service improvement.** The use of content data is of central importance, as many types of value-added services, from spell-checking to "attachment checking" and services that recognise and populate calendars with proposed appointments, all rely on artificial intelligence ("AI") scanning of content data, as well as metadata. Subjecting this type of data to stringent consent requirements is not consistent with the GDPR as communications data is not specified as "sensitive personal data" under Article 10 of the GDPR. Had the GDPR considered either category of electronic communications data to be sensitive, it would have said so explicitly.

In addition, Article 6 should be amended to clarify that any service provider may, if they meet the conditions of Article 6, process electronic communications data. While Article 5 applies to all parties, Article 6 remains narrowly drafted to enable processing only by electronic communications service and network providers. This narrow scope for Article 6 would leave out cybersecurity and other digital infrastructure providers who would be prohibited from processing under Article 5, but who are neither type of provider, and so could not process electronic communications data – despite their legitimate need to do so. Article 6 should be amended to enable processing by these parties also. It should also be further clarified that in cases where a legal person has subscribed to an electronic communications service, the legal entity is the end-user, and thus entitled to give consent (e.g. if such a service is used in a business context).

Question 2 – Do you consider the approach concerning the protection of terminal equipment and privacy settings (art 8 and 10) to be an acceptable basis to move forward?

While the Bulgarian Presidency text recognises the importance of permitting the deployment of security updates, the current Council text does not go far enough to recognise other legitimate purposes for operators to interact with terminal equipment. **In particular, Article 8 should be further amended to ensure that security updates that are prospective – e.g., upgrades to current practices that are not yet immediately "necessary" – are permitted**, as well as the activities necessary to both plan and implement those updates. It is also important that service providers be able to provide automatic security updates to all users. Allowing users to opt out of these important updates could lead to fragmentation of the ecosystem, with some users still using vulnerable older

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

versions of services – eroding security for all users. This is especially critical if terminal equipment is used in the employment context. It must be clarified that the employers are the end-user, and not the individual employees.

We also continue to support limiting Article 10 to web browsers only, in order to ensure clarity for stakeholders. Further amendments are also necessary to clarify that companies will not be required to produce new software for the huge multitude of different operating systems and devices that they have released in the past, particularly if they have discontinued support for those systems and devices.

Question 3 – Do you think that the latest compromise proposed by the Presidency is a future-proof approach and achieves the necessary balance between the protection of citizens data (or sensitive data) and the competitiveness of the European industry in providing innovative services?

We strongly believe that the current approach fails to strike the right balance. BSA recognises the fundamental importance of user privacy and data protection and have invested heavily in protective features across their services. However, at the same time, we stress that the future competitiveness of the European digital economy, and indeed of our members, *depends on innovation*. Other major markets have, while still protecting user privacy, not imposed analogous restrictions on the use of communications data.

The current Presidency compromise does not sufficiently recognise the need for innovation. The innovation that is threatened by the current draft ePR is **not about targeting ads or profiling users** – it is about *enabling AI to help users do more with better services and value-added features*. For example, our members are developing, and have launched, tools like real-time translation and voice recognition, based on the use of content and metadata. These features are positive for users as they make technology more accessible and have helped usher in new European users into the modern digital economy. We stand only at the cusp of the new machine learning revolution, and there are far more benefits to come. The question, however, is **whether those advancements will be permitted, or developed, in Europe.**

While our members continue seek more scope for innovation, this does not mean they do not value confidentiality or privacy. Any use of machine learning and AI in relation to communications data will already be governed by the GDPR – the most stringent and robust data protection framework in the world. The risk remains that the ePR will further restrict what is possible under the GDPR, in particular by over-relying on user consent. This will impose further significant costs on businesses before they have even finished grappling with the GDPR's extensive new requirements.

We have also voiced concerns about the impact of numerous provisions of the draft ePR on legitimate online business models. The Presidency has sought to address these concern, and for that we are grateful. Nevertheless, the scope for many popular services will be constrained, or simply unprofitable, under the current draft of the ePR – and, just as troubling, service updates designed to improve services will also be hindered.

For these reasons, we believe Member State should **continue working to further improve the draft ePR** to ensure Europe's future digital competitiveness.

[i] *BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With offices in Brussels, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.*
BSA's members include: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, Box, CA Technologies, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, Intuit, Microsoft, Okta, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Trend Micro, Trimble Solutions Corporation, and Workday.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48