Brussels, September 2017

BSA | The Software Alliance's position paper on the EU ePrivacy Regulation

BSA | The Software Alliance ("BSA")[1], the leading advocate for the global software industry, welcomes the opportunity to provide its views on the European Commission's proposal for an ePrivacy Regulation ("ePR"). BSA members share a deep commitment to digital privacy and take their commitments to protecting the confidentiality of electronic communications seriously. Many of our members have pioneered new methods of protection, including enhanced encryption measures. These protections, and more fundamentally the trust that they engender, are the bedrock of digital commerce.

We are concerned that the draft ePR – unlike the more principles-based approach of traditional European data protection laws – sets out wide-reaching and prescriptive rules, providing for only a small number of narrow exceptions. This approach will have a serious impact on innovators seeking to develop, experiment, and enhance both new and existing digital products and services.

These consequences risk having a real cost for the European economy. Software today contributes as much as 7% of existing EU GDP[2]. If promising technologies are supported, we expect this contribution to EU GDP to increase. However, this growth could be lost without the proper legal framework to enable it. This will particularly be the case for many of the most promising technologies of tomorrow, including IoT products, self-driving cars, machine-learning software, artificial intelligence, and digital personal assistants.

We encourage the EU's co-legislators to not only think of how to regulate today's technology, but also to consider how the draft ePR can be revised to *enhance* the ability for Europeans to innovate, while at the same time protecting fundamental rights. We would like to bring to your attention the following issue-specific points, which we believe can positively impact the creation of the technology of tomorrow:

1. **Machine-to-Machine ("M2M") Communications** – While the ePR aims to protect the fundamental rights of natural person's, in many cases M2M communications have no connection to a natural person's privacy or confidentiality. Consequently, M2M

[1] *BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the internationals marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, 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, CA Technologies, CNC/Mastercam, DataStax, DocuSign, IBM, Intel, Intuit, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Tend Micro, Trimble Solutions Corporation, and Workday.

[2] *http://www.softwareimpact.bsa.org/eu*

Avenue des Arts 44
1040 Brussels
Belgium

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

communications with no connection to a natural person's privacy or confidentiality should fall outside of the scope of the ePR.

2. **Alignment of Definitions** – Including 'ancillary communications services' into the scope of the ePR risks bringing the Regulation out of alignment with the European Electronic Communications Code. This will create unnecessary confusion for software developers. To avoid the creation of conflicting regulatory compliance regimes, ancillary communications services should be excluded from the scope of the ePR.

3. **Data '*in Transit*' vs. Data '*at Rest*'** – The ePR should seek to fully align with the GDPR. As the GDPR applies to data '*at rest'*, the application of the ePR should remain limited to data '*in transit'* focusing specifically on the prohibition of conduct such as the unlawful interception and scanning of communications transmissions.

4. **Scope of Article 6** – Many service providers that handle communications data may be unable to benefit from the processing exceptions found in Article 6 as they will likely not be classified as electronic communications services or electronic communications networks. This will lead to a prohibition on the processing of communications data for many ethical service providers. To avoid such a framework, the scope of Article 6 should be expanded so that the narrow exceptions of the ePR are available to all end-users processing communications data.

5. **Legal Basis for Processing** – The ePR's strict reliance on end-user consent for the processing of communications data will have a disproportionately negative impact on software innovation. The ePR should seek to provide additional flexibility for the processing of communications data through the introduction of a 'legitimate interest' legal basis.

6. **Law Enforcement Access to Data** – The ePR expands the manner in which Member States can restrict the right to confidentiality. Such an expansion risks eroding the trust of EU citizens. To avoid such an erosion, any restrictions to the rights found in the ePR should be strictly limited to what is necessary and proportionate in a democratic society.

7. **Web Audience Measuring** – The ePR risks expanding existing 'cookies rules' despite a recognition that today's framework does not serve consumers well. To avoid this, the ePR should clarify that web measurement by third parties acting on behalf of publishers is permitted under Article 8.

8. **Software Obligations** – In an attempt to address the problems stemming from the existing 'cookies' framework, the ePR seeks to impose unnecessary design requirements on all software, including those which have little to do with 'cookies'. To avoid the creation of blanket software mandates, the ePR should clarify that the obligations in Article 10 apply only to web browsers.

Avenue des Arts 44
1040 Brussels
Belgium

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

9. **Data Breach Notification** – An obligation on electronic communications services to notify data breaches would largely overlap with the notification requirements found in the NIS Directive, GDPR and European Electronic Communications Code. To avoid regulatory confusion and over-reporting, Article 17 should be deleted.

Issues and BSA Positions

1. Machine-to-Machine ("M2M") Communications

Under Recital 12 of the draft ePR, the Regulation is scoped to apply to the "*transmission of M2M communications*." We believe this **scope applied to M2M communications is too broad**. The purpose of the draft ePR, as set out in Recital 1, is to protect the fundamental rights and freedoms of natural person's in the provision and use of electronic communication services ("ECSs"). Yet in many cases, M2M communications have no connection to a natural person's privacy or confidentiality, particularly in business-to-business ("B2B") scenarios.

Business Example: A system that regulates the height of mechanical levees and flood defences based on automated measurements of upriver water flow. In such an example, communications between the sensors that measure water flow and the machines that control the levee and flood defence positions occur between machines – with no implications on the privacy of a natural person. Under the draft ePR, such communication would fall within scope of the law, requiring party's other than the "end-users" (e.g. local authorities or emergency planning agencies) to either not process the relevant communications data, or seek to find a basis for processing the data under Article 6.

Recommendation: We recommend that M2M communications between machines operated by one or multiple organizations – rather than individuals – should **fall outside of the scope of the ePR**. This could be accomplished through a clarification to the scope of the ePR (Article 2 and Recital 12). Alternatively, the definition of "end-user" (Article 5) could be clarified to ensure that M2M scenarios involving two businesses (or a single business, with multiple operators and machines) – and any third party acting on their behalf (e.g. data processors) – involve only "end-users".

2. Alignment of Definitions

The draft ePR aims to align the definition of an ECS with the definition found in the draft European Electronic Communications Code ("EECC"). However, despite this objective, the draft ePR expands the definition found in the EECC, adding in Article 4(2) that ECSs include "*services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service"* – known as ancillary communications services.

This addition brings the draft ePR out of alignment with the draft EECC, which is likely to create regulatory confusion. The inclusion will significantly increase the compliance burden in the software and application development communities. Consequently, it will have a **real effect on**

Europe's ability to create successful technology start-ups as many information society services will be faced with conflicting compliance provisions**.**

Business Example: A two-person start-up that seeks to develop an application for a service that provides baby sitters at the touch of a button. If this application also includes a way for the user to *communicate* with the baby-sitter, it would fall within the scope of the draft ePR. As a result, it may become difficult (or impossible) for the start-up to analyse usage data, which when aggregated, could reveal important usage patterns and trends that help developers anticipate periods of high demand on their services. Understanding such data can make the difference between the application being reliable, or being abandoned by its user's due to (unavoidable) downtime/slow response times.

Recommendation: We recommend that ancillary communications services be **excluded from the scope of the ePR**. The EU's co-legislators should seek to align the draft ePR with the draft EECC rather than create conflicting regulatory regimes.

3. Data '*in Transit' vs. Data 'at Rest'*

Under Recital 15 of the draft ePR, the Regulation notes that the prohibition on processing of electronic communications data without a legal basis in Article 5 should apply only to data "*in transmission*". This Recital is consistent with the need to ensure that the ePR prohibits conduct such as interception, scanning, etc. of communications "*in transit*." We believe that this is a **necessary component of the law to uphold trust in digital communications**.

However, the limitation set out in Recital 15 is not properly reflected in Article 5, which risks incorrectly expanding the scope of the ePR to communications data "*at rest*" (i.e. before and after the transmission of communications). The reference to "*processing*" in Article 5 – which does not exist in the current ePrivacy Directive ("ePD") – as distinct from other activities (e.g. listening, tapping, monitoring, and scanning) adds to the likelihood that Article 5 could be **misinterpreted as also applying to data "*at rest.*"**

Business Examples: Many digital players deliver services through the processing of electronic communications data "*at rest*". They do so by collating communications after they have been sent into a single repository so that the recipient can read the communications data on multiple devices. They also scan the content of a communication to 'bring to the surface' certain content through notifications (e.g. recognising an airline ticket has been sent to the user and then notifying the user when their flight is set to depart). Digital players also enhance the communications experience for users through spell checks or retrieving past conversation threads across devices, to more sophisticated uses such as processing of communications post-transmission to suggest specific actions across other information society services (e.g. personal assistants).

For all the above examples, the General Data Protection Regulation ("GDPR") applies directly to the processing – ensuring that it can only be carried out subject to the limitations and restrictions

of the law and in full respect of the fundamental rights of data subjects. We firmly believe there is **no need for added restrictions on such types of data processing**.

Recommendation: We recommend that Article 5 be amended to state explicitly that the **ePR is limited to data "*in transit*".** In addition, as the GDPR applies to personal data "*at rest*," we also recommend the **deletion of Article 7 to avoid unnecessary overlaps**. Such a deletion would not result in a 'gap' in protection for users, because the GDPR would still apply to the processing of any "*at rest*" communications data. Without such a deletion, we risk creating a legal framework where a user's photo taken and stored locally on their phone would be subject to a different level of protection than the very same image if it was downloaded from the web. In both instances, the rules should be consistent and as such, the GDPR should be the sole legal framework that users and software developers need to consider in such situations.

4. Scope of Article 6

In the draft ePR, Article 6 provides for only narrow exceptions to the overall prohibition of processing electronic communications data set out in Article 5. Moreover, the draft ePR only allows ECSs and electronic network providers ("ECNs") to invoke the narrow exceptions set out in Article 6. This is problematic as many service providers that handle communications data may not be classified as ECSs or ECNs and as such may be unable to benefit from the exceptions found in Article 6.

Business Example: A virus detection software provider, which scans communications data for malware and other malicious material. Virus detection software providers may not always be classified as ECSs or ECNs meaning that they would not benefit from the narrow exceptions for processing electronic communications data set out in Article 6. Such a situation would reduce data security and protection for users.

Recommendation: We recommend **broadening the scope of Article 6 so that the narrow exceptions are not only available to ECSs and ECNs**, but to all other parties (i.e. end-users) that are subject to the prohibition in Article 5.

5. Legal Basis for Processing

BSA is concerned that even when an entity falls within the scope of Article 6 and can benefit from the exceptions for processing communications data, the grounds are so narrow that they will have a **disproportionately negative impact on software innovation in Europe**. While Article 6 – specifically Article 6(3)(a) and (b) – would permit the *provision* of services (with end-users' consent), we fear the *development* of future features could be prohibited as product development involves the processing of the content of communications *sent* to an organisation's users from end-users of services offered by other organisations. An organisation developing new features has no possible way to obtain the consent from the *sender* as it has no relationship with these users. As a result, an organisation cannot obtain the consent of *all* end-users "concerned" under Article 6(3)(b). This will have a **direct impact on innovation**.

Business Examples: A company is seeking to improve a feature that removes spam messages through a spam filter or a company is developing a new feature that automatically flags communications that contain requests for a response from a user (e.g. meeting requests). In both such instances, the features benefit the users, but Article 5 would prohibit such processing and Article 6 would provide no ground that would permit such processing.

Recommendation: We recommend the **inclusion of a 'legitimate interests' legal basis into Article 6(2) and Article 6(3)**, consistent with the legal ground in the GDPR. Such a legal basis would not "trade away" or compromise on privacy as it can only be a lawful ground for processing where the rights and interests of individuals would not be potentially infringed. This legal basis ensures that the sensitivity of the relevant data is considered before processing is permitted. Moreover, it also encourages organisations to implement extensive safeguards – ranging from encryption to anonymization – to protect data subjects. We also recommend the **inclusion of "compatible" further processing language into Article 6(2) and Article 6(3)** in line with Article 6(4) of the GDPR as well as amendments to Article 6(1)(b) and Recital 16 to explicitly permit processing for detecting and preventing spam and other illegal content.

6. Law Enforcement Access to Data

BSA's members recognise the increasing challenges that law enforcement authorities must navigate in today's world. BSA shares a commitment to ensuring that authorities have the tools and information needed to fight crime and provide citizens with security. However, we are not convinced that the obligations placed on ECS providers in Article 11 are the correct way to facilitate such cooperation.

While Article 11 largely preserves the framework established by Article 15 of the ePD, it also expands the manner in which Member States can restrict the rights provided for in Articles 5 to 8 of the draft legislation. The direct reference to Article 23(1)(a) to (e) of the GDPR in Article 11(1) represents a **clear expansion of the restrictions found in the ePD to broadly worded general public interests** such as "*important economic or financial interests of the Union"*. This expansion will lead to an erosion of trust amongst EU citizens and have a negative impact on Europe's digital economy. Any restrictions to the rights found in Articles 5 to 8 should not be based on broad principles but instead limited to what is necessary, appropriate and proportionate in a democratic society.

BSA is also concerned that Article 11(2) of the draft ePR, which would require ECS providers to "*establish internal procedures for responding to requests for access to end-users' electronic communications data*", **lacks a clear material threshold.** This provision is likely to unnecessarily burden many ECS providers, especially those which do not have a history of receiving requests for access to end-users' data from law enforcement authorities. While many large multinational online service providers already typically maintain relevant procedures, and publish aggregate information how they respond to law enforcement requests, we question whether there is truly a need for all ECS providers to require such procedures.

Furthermore, Article 11(2) would also require ECSs to provide data protection authorities ("DPAs"), on demand, with "*information about those procedures, the number of requests received, the legal justification received and the response.*" This **obligation does not properly take into consideration the potential legal disclosure restrictions that can sometimes be placed on ECS providers** by law enforcement authorities or tribunals. Consequently, any response to DPAs should be governed in accordance with the legal requirements of the Member State where the ECS provider has its main establishment and should avoid placing entities in a conflict of law situation.

Recommendation: We recommend the **deletion of the reference to Article 23(1)(a) to (e) of the GDPR in Article 11(1)**. This will ensure that the ePR does not unnecessarily expand the justifications that can be used by Member States to restrict the rights provided for in Articles 5 to 8.

Article 11(2), which pre-empts the European Commission's legislative proposal set for early-2018 aimed at addressing cross-border access to electronic evidence, should be **clarified so that ECS providers may only responds to disclosure requests in accordance with the legal requirements of the Member State where the provider has its main establishment**.

7. Web Audience Measuring

We welcome the European Commission's recognition that the existing "cookies" framework does not serve consumers well by overwhelming them with requests for consent. We also welcome the addition in Article 8(1)(d) of an exception to help enable web audience measuring as this activity is necessary for the design of modern interfaces which enable website usability and accessibility.

However, despite the positive intentions of the European Commission, we remain concerned that the draft ePR will retain – and expand – the existing "cookies rule" set out in the ePD. When considering Article 8(1)(d), it remains unclear as to whether web measurement is permitted under the exception only if carried out *by* a first party website publisher, or also by third parties *on the publisher's behalf*. This ambiguity is problematic given that most web publishers *do* rely on third parties acting on their behalf to provide web measurement tools and technologies. This allows publishes to focus their efforts and limited resources on bettering their services and making them more secure. However, the draft ePR would likely require publishers to develop, test and implement their own web measurement tools, rather than outsource that activity to existing platforms.

Recommendation: We recommend that the ePR clarify that **web measurement by third parties acting on the publisher's behalf is also permitted under Article 8(1)(d).** This clarification would help online publishers continue to innovate and improve interfaces in the future while avoiding penalising smaller publishers. We also recommend the introduction of a new exception in cases where data is immediately anonymised after it is collected. Such an exception would not

compromise privacy, ensure consistency with the GDPR, and allow for innovation by enabling greater use of statistical and aggregated data by web publishers.

8. Software Obligations

BSA takes note of the draft ePR's efforts to address the problems stemming from the existing "cookies" framework by attempting to "centralise" the "cookies consent" mechanism through browser settings. This is set out in Article 10 which requires makers of "*software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet*", to provide for an appropriate setting through which users can express consent.

However, we believe that the **provisions of Article 10 are too broad** as they could cover many types of software – such as VoIP-based messaging software – which have little to do with "cookies" and would either not be able to develop such a setting or provide services where such a setting would be irrelevant.

Recommendation: To ensure that Article 10 is proportionate and avoids imposing design requirements on all software, we recommend **clarifying that the obligations in Article 10 apply only to web browsers.** By limiting Article 10 to web browsers, the ePR would avoid creating a scenario where a user, acting through multiples layers of software (browser, operation system, application, etc.), sets the relevant setting in each layer to different, potentially incompatibly configurations.

We would also recommend the removal of the unclear statement in Recital 22 which states that "*the choices made by end-users when establishing its general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties*." The basic position under the ePR is that third parties are prohibited from placing or reading cookies on a user's device without consent under Article 8. Suggesting in a Recital that the browser setting is *in any case* binding and somehow "enforceable," regardless of whether consent has been obtained through other means, goes against this basic position and is likely to confuse entities.

9. Data Breach Notification

The obligation on ECSs to notify data breaches set out in the ePD was an important obligation to drive consumer confidence. The ePD led the way in developing the concept of data breach notifications and made a valuable contribution to the maintenance of cybersecurity in Europe's digital economy. Our members continue to **recognise the value of data breach notifications and the legal requirements mandating them.** This is properly reflected in the GDPR through the introduction of comprehensive notification requirements.

Considering the GDPR, we believe the inclusion of Article 17 in the ePR, which requires ECSs to notify end-users where *"particular risks that may compromise the security of networks and ECSs arise,*" is unnecessary. The need for network and ECS security is already to a large extent

maintained through the 2002 Framework Directive, which requires undertakings providing public communications networks or publicly available ECSs to notify the competent regulatory authorities in cases of breaches of security or loss of integrity that has a significant impact on the operation of networks or services. This provision is set to be further expanded in Article 40 of the draft EECC. Any accompanying provision within the ePR will only lead to confusion and double-reporting of breaches.

Recommendation: We recommend that Article 17 and Recital 37 be deleted.

For further information, please contact:
Thomas Boué, Director General, Policy – EMEA
thomasb@bsa.org or +32.2.274.1315