Brussels, February 2019

Outstanding issues to be resolved for a balanced ePrivacy Regulation

Background

On 15 February 2019, in order to facilitate further discussion among the Council, the Romanian Council Presidency published a revised text of the draft ePrivacy Regulation ("ePR") (the "Presidency Draft").

BSA | The Software Alliance ("BSA")[1], the leading advocate for the global software industry, has already voiced its concerns[2] on the status of the negotiations, and we continue to believe that further discussions are needed in order to consider fully the potential impact of the ePR on EU consumers, businesses, and suppliers. We encourage the Council to continue evaluating the proposal carefully rather than rushing to finalize the text. As we have sought to act as a trusted partner throughout the legislative discussions, we set out below some of the reasons why we believe the draft ePR remains in need of further refinement and suggest some constructive ways in which these outstanding issues might be resolved without undermining the fundamental objectives of the draft legislation.

1. Article 6 – Scanning for Child Sexual Exploitation and Abuse Imagery

BSA has consistently advocated for language that will enable service providers to scan proactively for and remove child sexual exploitation and abuse imagery. We therefore welcome the proposed amendments to Recital 26 and Article 6(1)(d) and Article 6(1a) designed to enable providers to continue their efforts to address and remove this unlawful and highly objectionable form of content.

Nevertheless, the Presidency Draft is incomplete and would not give providers the ability to combat such content effectively. In particular, the Presidency Draft does not expressly permit processing for the purpose of *reporting* such content, once detected, to relevant authorities. Also, the Presidency Draft does not appear to permit "analysis" of communications content for this purpose, or to store copies of such content, which could prevent effective evidence-gathering by legal authorities and potentially conflict with providers' retention obligations. We also question the need for providers undertaking these activities to carry out a data protection impact assessment and prior consultation with supervisory authorities. Taken together, these requirements will substantially hinder the ability of providers to identify and remove child sexual abuse and exploitation imagery effectively, and we urge the Council to reconsider them.

---

[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, Akamai, Apple, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, Siemens PLM Software, Slack, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[2] *Joint industry letter on EU ePrivacy Regulation – 4 December Telecommunications Council (link)*

Avenue des Arts 44
1040 Brussels
Belgium

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

In addition, BSA encourages the Council to extend these amendments to Article 6(1) to also cover terrorist content. The Council is certainly aware of efforts at both the EU and Member State levels to encourage, and even require, online service providers to identify and remove terrorist content quickly. Those efforts could be thwarted if providers face a risk of liability under the ePR for undertaking such efforts.

2. Article 6 – Processing Content Data for General Training and Improvement of Machine Learning Algorithms

BSA welcomes amendments to provide additional flexibility to providers seeking to process communications metadata under Article 6(2). We recognise the sensitive nature of electronic communications data, and in particular of electronic communications content data. However, we continue to believe that the strict prohibitions placed on the processing of electronic communications content data within Article 6(3) will have a direct negative affect on the ability for software companies to improve machine learning algorithms and deploy new technologies based on artificial intelligence ("AI") across the EU. Given the nature of these technologies, a regulatory framework on the processing of content data that is built solely upon the consent of the end-user may prevent Europe from taking full-advantage of AI, even when all appropriate steps are taken to anonymise and minimise data processing. This lack of flexibility within the Council's current draft text fails to correspond with the stated objectives of both the EU and Member States within the field of AI.

In practical terms, the scope of the Regulation does not provide legal certainty for several activities involving "emerging technologies". For example, smart connected cars which exchange information with other compatible devices (e.g. about a rapid break manoeuvre or with smart traffic signs), establish an electronic communications network, therefore would fall under the scope of the Regulation. In such case, as in many similar ones, the Regulation fails to clearly indicate which entity would be required to give consent. We encourage the Council to adopt amendments that would permit processing of content data for clearly legitimate, pro-consumer and otherwise lawful purposes, such as for purposes of research and development and the development of AI and other emerging technologies.

3. Article 8 – Software Updates

BSA welcomes the improvements made to Article 8. However, it remains unclear how software updates will be delivered to the terminal equipment of end-users if the text of Article 8 as set out in the Romanian Presidency text were to come into force. We are particularly concerned that the exception to the consent requirement remains focused on those software updates that contain a security component. Even where software updates are not "necessary" for security, software that is not routinely updated may create security vulnerabilities, and may impair other important aspects, such as its usability, accessibility, and other functionalities. Limiting the exception in Article 8(1)(e) to software updates that are "necessary for security reasons" only would not allow service providers to fully address the challenges caused by outdated software, as this cannot be done by security updates alone. Outdated software requires updates to address 'bugs' along with performance, design and functionality issues. Security updates are not meant to solve such

issues and consequently, updates are often bundled to address a variety of issues, including compliance with legal obligations (e.g. introduction of more granular cookie controls).

We propose the following language as amendments to the Presidency Draft to solve this issue (with our amendments proposed in bold and strikethrough):

> *Article 8: 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:*
> *. . . .*
> *(e) it is necessary for a software update provided that:*
>
> *(i) such update is necessary for security**, usability, accessibility, or other functionality-related** reasons and does not in any way change the privacy settings chosen by the end-user **if that would result in the end-user having a lower privacy standard**, and*
>
> *(ii) the end-user is informed in advance each time an update is being installed **except where this is not possible due to the lack of a user interface~~, and~~***
>
> ***~~(iii) the end-user is given the possibility to postpone or turn off the automatic installation of these updates~~**.*

Consistent with these amendments, we also urge the Council to adopt corresponding changes to the final paragraph of Recital 21a, and in particular to remove the sentence that reads: "Software updates that do not exclusively have a security purpose, for example those intended to add new features to an application or improve its performance, should not fall under this exception."

Moreover, in a business environment, the current formulation of Art. 8 would cause significant practical issues, some of which may be insurmountable. The language in Art. 8 – and in broader terms in the whole Regulation – should consider the instances in which electronic communication services are used to carry out business-related (not private) communications of a legal entity. In such cases, providers should be able to obtain consent from the legal person or a competent individual acting on behalf of the legal entity. This is especially critical if terminal equipment and electronic communication services are used in the employment context for work purposes. It must be clarified that the employers are the end-user, and not the individual employees. This is important for a number of business processes. For example, if software on terminal equipment (e.g. smart phones, tablets, computers, control units) is used for business reasons (e.g. business applications for sellers, software to control production lines), the "end-user" with the authority to decide on updates (functional and security) should be the legal entity, i.e. the employer. Otherwise, each individual employee could separately decide which version of the software to use, which would put the business at risk of not having access to the latest business processes

or security requirements. To address this issue, the draft Regulation should therefore be amended to clarify that, where the end-user is a legal person, that legal person's consent satisfies any end-user consent requirements set out in the Regulation. Although we note the amendment to Article 4a, that provisions relating to consent provided for under the GDPR shall apply "*mutatis mutandis*" to legal persons as they do to natural persons, this text should be clearer in stating that providers can satisfy the end-user consent requirements set out in the ePR by obtaining the consent of the relevant business entity, and do not also need the consent of individual employees of that entity. Accordingly, we would also encourage the Council to amend Recital 19b as follows and add a Recital 23a (our proposed amendments in bold and strikethrough):

> *"(19b) Providers of electronic communications services may, for example, obtain the consent of the end-user for the processing of electronic communications data, at the time of the conclusion of the contract, and any moment in time thereafter. In some cases, the legal entity subscribed to business-related electronic communications services* ***, for instance for the professional communication of employees.*** *~~may allow a natural person, such as an employee, to make use of the service.~~ In such case, consent* ***may*** *~~needs to~~ be obtained from the* ***legal person concerned, and not necessarily from the individual user*** *. ~~the individual concerned.~~"*
>
> *"****(23a) Terminal equipment which is used for business reasons, such as computer, laptops, tablet computers or smart phones, for example to control production facilities and machines or to run business software, has to be automatically updated, maintained and managed to reflect the relevant business needs and to comply with information security requirements. In this context, the end-user is the legal person (employer), for example a company, who must give consent to the use of processing and storage capabilities of terminal equipment and the collection of information from terminal equipment.*"***

With regards to cybersecurity, we believe that the progress achieved in Recital 8 and in Article 2(2) subpoints (e) and (f) improve considerably the text and address the cybersecurity considerations BSA raised in the past.

We welcome the deletion of the wording "information society" in Art. 8(1)(c) as it allows for more flexibility in the provision of services. Similarly, to ensure a Regulation that addresses all cybersecurity concerns, we propose the deletion of the words "of information society services" in Article 8(1)(da). In some cases, it may be necessary to interact with the terminal equipment in order to protect it from malicious software/viruses and other attacks. These threats appear on the terminal device and are not necessarily linked to a particular information society service. For example, they could be related to a supply chain attack (e.g., installation of software or hardware that is already compromised). In the current formulation of the Regulation, it will not be possible

for cybersecurity providers to detect the compromise of terminal equipment through their threat intelligence network (e.g. the Mirai botnet spread from thousands of infected consumer IoT devices, it would have been almost impossible to detect where the attacks are coming from if the current wording in Art 8 was enforced). This is particularly relevant in light of the discussions happening in Europe about equipment manufacturers outside the EU.

4. Article 10 – Privacy Settings

BSA also welcomes the decision by the Romanian Presidency of the Council to confirm the deletion of Article 10. However, as some Member State delegations supported the re-introduction of Article 10 into the Council's draft text, questions remain as to how to address the technical limitations of web browsers (should this issue be discussed further). BSA continues to stress that while web browsers can successfully block cookies, they do not know how to distinguish between the purpose of each specific cookie. Only publishers who deploy cookies are in a position to know the purpose of each cookie and their relationship to data processing. BSA remains highly sceptical as to how any version of Article 10 will work in practice across not just web browsers, but software more broadly. BSA strongly supports the principle of effective users' control over their data, complemented with the accountability principle, both of which the General Data Protection Regulation already addresses. Consequently, we encourage the Council to preserve the deletion of Article 10.

5. Article 11 – Data Retention

BSA notes that throughout the discussions on the draft Regulation within the Council, limited time has been spent discussing the impact of Article 11 and the ability for Member States to restrict the rights set out in Articles 5-8. Of particular concern is the interplay between Article 11 and the issue of "data retention", which was highlighted by the Austrian Presidency of the Council in its Progress Report. BSA believes that this issue requires more debate within the Council in light of the detailed case law (*Tele 2 & Breyer*), which emerged following the entry into force of the existing ePrivacy Directive.

6. Article 11 - Encryption

Similar to the above, BSA notes that the European Parliament, in its negotiating position, has shown a clear preference for electronic communications service ("ECS") providers to use state of the art technical measures, including the end-to-end encryption of electronic communications data to guarantee the confidentiality and integrity of end-users' communications. BSA believes that there is a clear friction between the position of the European Parliament and the Council's draft text in relation to the extension of surveillance practices. This issue should be further discussed and resolved prior to entering into negotiations with the European Parliament in an effort to avoid a stalemate.

7. Machine-to-Machine Communications

BSA member companies continue to heavily invest in software services that enable to smooth functioning of machine-to-machine ("M2M") communications. This technology includes a vast array of devices and services, which makes any one-size-fits-all regulatory approach challenging and difficult to implement. BSA continues to believe that the broadening of the scope of M2M

would mean that numerous products and services that contain built-in M2M communication features (e.g. automated supply chains and remote control or distance operation of machines) will be covered by the legislation, despite the intention of the European Commission and some Member State delegations to not do so. The inclusion of such products and services into the scope of the future regulatory framework would be inconsistent with the purpose and objectives of the draft ePR and would lead to unworkable obligations while potentially rendering standard processes and developments of industry 4.0 impossible. Despite attempts in the Presidency Draft to clarify the provisions on M2M communications, including in Recital 12, the current proposed text still fails to provide future-proof rules.

Including M2M – even to the extent set out in Recital 12 – could require any legal and natural persons that are owners of connected devices to express consent according to the draft ePR rules for the processing of electronic communication data for both personal and non-personal data. Additionally, each time a device enters the range of a new sensor network and tries to exchange data with other external sensors, (e.g. data centers' environmental sensors) consent would be required. BSA supports measures to protect the confidentiality of interpersonal communications and/or communications concerning machines transmitting personal data, however, M2M communications that do not carry personal data and are not conveyed between individuals should not be subject to data protection or privacy rules. The amendments reflected in the Presidency Draft do not address these concerns. Accordingly, we urge the Council to undertake further discussions with all relevant stakeholders to ensure that the final text takes into consideration the diverse set of technologies that would be affected by the current draft ePR text.

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